Intrusion Prevention System (IPS)

https://campus.barracuda.com/doc/73719232/

The Intrusion Prevention System (IPS) actively monitors local and forwarding traffic for malicious activities and can also block suspicious traffic. The IPS engine analyzes network traffic and continuously compares the bitstream with its internal signatures database for malicious code patterns. You can create, edit, and override default and custom IPS signature handling policies. After configuring your IPS policies, you can also apply them to your access rules.

IPS Features

TCP Stream Reassembly

The firewall engine provides support for TCP Stream Reassembly (SRA). In general, TCP streams are broken into TCP segments that are encapsulated into IP packets. By manipulating how a TCP stream is segmented, it is possible to evade detection. For example, by overwriting a portion of a previous segment within a stream with new data in a subsequent segment. This method allows the hacker to hide or obfuscate the network attack. The firewall engine receives the segments in a TCP conversation, buffers them, and reassembles the segments into a correct stream. For example, by checking for segment overlaps, interleaved duplicate segments, invalid TCP checksums, and so forth. Afterwards, the firewall engine passes the reassembled stream to the IPS engine for inspection.

URL Obfuscation

The IPS engine provides various countermeasures to avert possible network attacks based on the following URL encoding techniques:

- Escape encoding (% encoding)
- Microsoft %u encoding
- Path character transformations and expansions (/./ , //, \ )
- Premature URL ending
- Long URL
- Fake parameter
- TAB separation
- FTP Evasion

The IPS engine is able to avert FTP exploits where the attacker is trying to evade the IPS by inserting additional spaces and Telnet control sequences in FTP commands.

TCP Split Handshake

The IPS engine provides an evasion countermeasure technique that is able to block the usage of TCP

split handshakes attacks. Although the TCP split handshake is a legitimate way to start a TCP connection (RFC793), it can also be used by hackers to execute various network attacks by gaining access to the internal network by way of establishing a trusted IP connection, thus evading firewall and IPS policies.

Configuring and Managing IPS

For step-by-step instructions on how to configure and manage IPS, see the following articles: